Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan:
MinBZK

Via:
SG BZK

Van:
DGAIVD

Contact
T + 5.1.2.e
F + 5.1.2.e

Ons kenmerk
9b832ade-or1-1.2

Datum
22 april 2024

Bijlagen
0

memo

BNC-fiche aanbeveling routekaart voor post-quantumcryptografie (PQC)

Aanleiding

- Op 8 mei bespreekt de BNC het fiche over de aanbeveling van de Europese Commissie over een routekaart voor een coördineerde uitvoering van de transitie naar post-quantumcryptografie.
- Om de AIVD penvoerder is voor het fiche, wordt de voorgenomen kabinetsinzet bij u getoetst.

Advies

- Instemmen met voorgestelde kabinetsinzet.

Kern

- BZK en J&V zijn de verantwoordelijke ministeries, gezien het voorstel overheidsorganisatie en andere kritieke infrastructuren betreft. Via de BNC is afgesproken dat BZK penvoerder is.
- Het doel van het voorgestelde initiatief is om de nationale transitieplannen naar Post-Quantumcryptografie gecoördineerd uit te voeren met behulp van een Europese routekaart ten behoeve van internationale interoperabiliteit.
- De voorgestelde kabinetsinzet is overwegend positief. Het kabinet verwelkomt het initiatief en het hierin beschreven plan van activiteiten.
- Wel acht het kabinet nadere uitwerking van de inhoudelijke scope noodzakelijk, bijvoorbeeld op het gebied van de wendbaarheid van systemen voor gebruik van nieuwe cryptografie (‘*crypto agility*’).
- Ook dient geborgd te worden dat de Europese routekaart in lijn is met de in Nederland lopende risicogebaseerde aanpak van de transitie naar Post-Quantumcryptografie.

Toelichting

Nadere analyse van het voorstel

- De Commissie herkent de urgentie voor de dreiging van de quantumcomputer op de vertrouwelijkheid van informatie en adviseert een spoedige transitie naar Post-Quantumcryptografie.
- De Commissie moedigt de Lidstaten aan om in onderlinge samenwerking een strategie en routekaart te ontwikkelen voor de adoptie van Post-Quantumcryptografie voor een gecoördineerde en gesynchroniseerde transitie onder de Lidstaten.
- Lidstaten worden aangemoedigd om hun acties te coördineren via een toegewijd Lidstatenforum. Het forum kan vertegenwoordigers bevatten

van nationale beveiligingsautoriteiten en cybersecurityexperts van nationale cybersecurityautoriteiten en ENISA.

- De routekaart moet als blauwdruk dienen voor bepaling van de nationale plannen voor transitie naar Post-Quantumcryptografie, of indien die plannen reeds bestaan, voor de afstemming ervan op de routekaart.
- De meerderheid van de voorgestelde acties in de aanbeveling is in lijn met staand Nederlands beleid. Waar het indruist tegen Nederlands beleid is in het ontwikkelen van een hybride oplossing van Post-Quantumcryptografie en *Quantum Key Distribution*. Het nationale beleidsadvies is de inzet van een hybride oplossing van Post-Quantumcryptografie gecombineerd met de huidige cryptografie. Dit geldt voor de door de Commissie genoemde sectoren zoals overheidsdiensten en andere kritieke infrastructuren, maar ook voor alle andere infrastructuren in Nederland.
- Een ander advies van de Commissie is het ontwikkelen van gemeenschappelijke Europese standaarden. Vanuit Nederland is het van belang dat vanuit dit advies de bestaande initiatieven van standaardisatieorganisaties worden gevolgd, zoals ISO en NIST. Hierbij is het belangrijk dat er standaarden ontwikkeld worden die breed onder de Lidstaten gesteund worden.

Krachtenveld

- Samen met Duitsland, Zweden, Frankrijk en Italië maakt Nederland deel uit van de *AQUA Reference Group*. Dit is een selecte groep landen die cryptoproducten evalueren voor gebruik in EU-verband ('tweedelandsevaluatie'). Namens Nederland neemt de AIVD deel aan deze groep.
- De *AQUA Reference Group* is tot op heden eensgezind over een gecoördineerde transitie naar Post-Quantumcryptografie.
- Enkele leden van de *AQUA Reference Group* hebben een gezamenlijk visie op de inzet van transitie naar Post-Quantumcryptografie eerder toegelicht in een *position paper*. In dit paper adviseren de leden meer onderzoek te doen naar de beveiligingsaspecten van *Quantum Key Distribution*, zodat deze technologie op langere termijn ook inzetbaar wordt. U heeft dit *position paper* op 16 februari aan de Kamer gestuurd.